

Judge Robert J. Bryan

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA,

Plaintiff,

v.

JAY MICHAUD,

Defendant.

NO. CR15-5351RJB

UNITED STATES' RESPONSE TO
ORDER COMPELLING DISCOVERY

The United States of America, by and through Annette L. Hayes, United States Attorney for the Western District of Washington, Matthew P. Hampton, Assistant United States Attorney for said District, and Keith A. Becker, Trial Attorney, hereby files this response to the Court's December 15, 2015, order compelling discovery (Dkt. 81):

A. Number of pictures, videos, and links

The Court first ordered the government to provide the defense with the number of child pornography pictures, videos, and links to pictures and videos that were posted on Website A between February 20 and March 4, 2015, "[p]rovided however, if the plaintiff cannot produce the exact picture, video and link totals listed above with reasonable effort, the plaintiff should provide a good faith estimate of the totals." Dkt. 81, pp. 1-3.

Website A was an online bulletin board through which users provided the content of the site by posting messages and/or replies to messages within categories set up by the site

UNITED STATES' RESPONSE TO DEFENDANT'S MOTION
TO DISMISS INDICTMENT (*United States v. Michaud*, CR15-5351 RJB) - 1

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

1 administration. In accordance with the site rules and guidelines, users generally posted textual
2 messages in which “preview” images (generally consisting of still frames taken from a video or a
3 selection of images) were embedded, and that included a link to a URL, the address of a website
4 or server at which the videos or images could be downloaded, along with any password
5 necessary to download and decrypt the videos or images.

6 During the course of the investigation of Website A, before and after its seizure, the FBI
7 expended significant efforts to document and capture as many of the images/videos posted in this
8 fashion by site users as practicable. Given the significant number of users and activity on the
9 website, it was not possible to capture all of that content. To access the images and videos, the
10 agents had to access the website or link contained in the message, download the files or a file
11 “archive” – that is, a compressed file containing numerous other files – and then enter a
12 password in order to access the files. This process could not be automated, meaning that it was
13 necessary for an agent physically to take these steps rather than simply direct a computer to do
14 the work. Moreover, images and videos that were made available by Website A users were
15 generally only available for a limited time. Thus, if the agents were not able to complete
16 accessing all of the website’s advertised materials at or near the time of posting, those materials
17 might no longer be available. With that understanding, we provide the following good faith
18 estimates based upon FBI agents’ downloads of files made available by the users of Website A
19 through their posts and through the seizure of data from the Website A image and file hosts.

20 Through the efforts described above, the FBI recovered approximately 48,000 images
21 and 200 videos that were made available by the site’s at least 184,000 users between the
22 inception of Website A in August 2014 and its seizure on February 20, 2015. In addition, the
23 FBI was able to recover approximately 9,000 images and 200 videos that were made available by
24 Website A users while it operated under FBI administrative control between February 20 and
25 March 4, 2015. The vast majority of those images/videos appeared to depict child pornography
26 or child erotica. In some instances, particularly with respect to sets of images pertaining to a
27 particular child, children were depicted in various states of undress progressing to nudity and/or
28 sexually explicit activity. This is common among child pornography images.

Website A users posted approximately 110,000 links on the website between August
2014 and February 20, 2015. During the period from February 20 through March 4, 2015,

1 Website A users posted approximately 13,000 links on the website. As noted above, links posted
2 by Website A users typically pointed either to encrypted archives containing multiple image or
3 video files of child pornography, or to particular image files depicting child pornography.
4 Although FBI cannot specify exactly how many images and videos were contained within each
5 of those encrypted archives, as noted above, FBI was able to recover approximately 9,000
6 images and 200 videos that were made available by Website A users while it operated under FBI
7 administrative control between February 20 and March 4, 2015.

8 **B. Views and downloads from February 20 through March 4, 2015**

9 The Court next ordered the government to provide the defense with the number of child
10 pornography pictures and videos that were viewed and downloaded from Website A between
11 February 20 and March 4, 2015, or a good faith estimate of these totals. Because of the manner
12 in which Website A works, it is not possible to give an exact total of child pornography images
13 or videos viewed or downloaded by site users during that time period. As noted above, Website
14 A was a bulletin board on which users posted messages with embedded links and preview
15 images. Another user may choose simply to view the preview image that is embedded on a web
16 page without clicking that image or taking an action that would be recorded by Website A.
17 Moreover, there are numerous ways for a user to save or download images contained on a
18 website such as Website A that would not be recorded by the website. For example, a user might
19 “right click” and save an image to the user’s computer. The user could also take a “screen shot”
20 of the computer screen, or go directly to the external website where linked images or videos were
21 contained by typing the URL for the site after leaving Website A, and then entering the
22 appropriate password, and downloading the images/videos. With that understanding, we provide
23 the following good faith estimates.

24 Information about the number of links Website A users clicked on between August 2014
25 and February 20, 2015, before the FBI was in administrative control of the website, is not
26 available. Between February 20 and March 4, 2015, Website A users clicked on approximately
27 67,000 unique links on the website. As explained above, links on Website A typically pointed
28 either to encrypted archives containing multiple image or video files of child pornography, or to
particular image files depicting child pornography. Of those 67,000 links, 25,000 were links to

1 image files, the majority of which appeared to depict child pornography. The remaining links
2 were to websites, which typically contained the sort of encrypted archives described above.

3 **C. Statistics concerning Website A usage between February 20 and March**
4 **4, 2015**

5 The Court next ordered the government to provide the defense with the number of
6 visitors to the site between February 20 and March 4, 2015, the number of total visits, and some
7 measure of the length of visits. Between February 20 and March 4, 2015, approximately
8 100,000 unique user accounts logged in to Website A, and there were approximately one million
9 total logins. An individual could have more than one user account on the site, so it is not clear
10 how many individuals this actually represents. Website A tracked total time spent on the site by
11 each user during the course of the user's membership. From the inception of the website in
12 August of 2014 until March 4, 2015, site data indicate that its more than 200,000 users
13 aggregately spent approximately seven million hours logged into the site. Based on available
14 data and with reasonable effort, the government cannot provide an estimate of the total or
15 average length of site visits between February 20 and March 4, 2015. Providing such figures
16 would require a manual review of every single session by every single site user in order to total
17 the amount of time spent during each session, and then average that amount of time. That
18 manual analysis has been done for Mr. Michaud (via data that have been provided to the defense
19 in discovery pertaining to his use of Website A) and shows that during his fourteen total sessions
20 on Website A between February 21, 2015, and March 2, 2015, Michaud spent approximately
21 sixteen-and-a-half hours on Website A for an average of 1.18 hours per visit. As previously
22 disclosed, Michaud spent a total of approximately ninety-nine hours logged into the site between
23 October 31, 2014, and March 2, 2015.

24 **D. Mitigation efforts**

25 The Court next ordered the government to provide the defense with a summary of any
26 measures that were taken by the FBI or other law enforcement entities to block access to the
27 pictures, videos and links available on or through the Website A between February 20 and March
28 4, 2015.

During the brief period when the FBI assumed administrative control of Website A, the
FBI did not post any images, videos, or links to images or videos of child pornography. Images,

1 videos and links posted by site users both before the FBI assumed administrative control and
 2 afterwards, generally remained available to site users.

3 While Website A operated under FBI administrative control, FBI Special Agents
 4 monitored all site postings, chat messages, and private messages twenty-four hours per day in
 5 order to comply with Title III monitoring requirements and in order to assess and mitigate any
 6 risk of imminent harm to children. In the event that FBI Special Agents perceived a risk of
 7 imminent harm to a child, agents took actions to mitigate that risk and immediately forwarded
 8 available identifying information, including NIT results, to the appropriate FBI office. Specific
 9 actions taken in any particular instance were tailored to the specific threat of harm. The
 10 particular actions taken by law enforcement agents in response to particular circumstances are
 11 protected by a qualified law enforcement privilege, which the United States hereby asserts. In
 12 particular, disclosure of this information at this point in time would alert subjects of ongoing
 13 investigations to the particular investigative techniques used by law enforcement in response to
 14 such circumstances, creating a risk that criminal suspects will recognize and circumvent such
 15 techniques in the future and leading to increased danger of harm to the public, including
 16 children. The risk of circumvention of an investigative technique if information is released has
 17 been recognized as a factor in applying law enforcement privilege to electronic surveillance. *See*
 18 *United States v. Van Horn*, 789 F.2d 1492, 1508 (11th Cir. 1986). In any event, no such actions
 19 pertained to any postings or messages involving the defendant's known username, Pewter.

20 **E. Reason for shutting down Website A**

21 The Court also required the government to produce the reasons the site was shut down on
 22 March 4 (rather than earlier or later). As the government explained to the two separate judges
 23 who authorized the NIT and the Title III authorization to monitor site users' communications, the
 24 fourteen-day period during which the FBI allowed the operation of Website A to continue was
 25 necessary in order to deploy the court-authorized NIT to identify users of this site who, like Mr.
 26 Michaud, used Tor to conceal their identity, location, and illegal conduct. Without using the
 27 NIT, the identities of the users of Website A would remain unknown because, unlike a non-Tor
 28 website, any IP address logs of user activity on Website A would disclose only Tor "exit nodes,"
 which could not be used to locate and identify the actual administrators or users of the site.
 Further, because of the unique nature of the Tor network and the method by which the network

1 routes communications through multiple other computers, investigative procedures that are
2 usually employed in criminal investigations of this type were tried and failed or reasonably
3 appeared to be unlikely to succeed.

4 The government demonstrated the necessity of the investigative strategy and technique
5 used in this investigation in the affidavit submitted in conjunction with its Title III authorization.
6 As the government indicated in that affidavit, agents considered seizing Website A and removing
7 it from existence immediately and permanently. In the judgment of law enforcement agents,
8 while doing so would have ended the trafficking of child pornography taking place via Website
9 A, it would have also prevented law enforcement from attempting to locate and identify its users,
10 who were the ones who possessed, and were distributing and receiving, those illicit materials. It
11 also would have frustrated agents' attempts to obtain information that could help identify and
12 rescue child victims from ongoing abuse. Accordingly, it was the judgment of law enforcement
13 that the seizure and continued operation of Website A, for a limited period of time, paired with
14 the court-authorized deployment of a NIT and monitoring of user communications, was
15 necessary and appropriate in order to identify Website A users. The judges who signed the NIT
16 warrant and Title III authorization obviously agreed.

17 To be sure, shutting down a facility such as Website A would have prevented its
18 unidentified users from continuing to post and disseminate child pornography through that
19 website, but it would not prevent those users from continuing to unlawfully possess and
20 disseminate child pornography by other means. Website A users engaged in that sort of activity
21 before the FBI seized and shut down Website A, and those users who were not identified and
22 apprehended undoubtedly continued to engage in that activity after Website A was shut down,
23 often through other online facilities. For instance, before the February 20, 2015, seizure of
24 Website A, it contained at least 184,000 active user accounts, 103,000 posts, and facilitated
25 access to thousands of images and videos of child pornography. There are currently child
26 pornography bulletin boards operating on the Tor network that are similar in structure and
27 function to Website A, that contain hundreds of thousands of user accounts, tens of thousands of
28 postings, and which facilitate access to thousands of images and videos of child pornography.
Law enforcement agents can view and document those websites, their contents, and the child
pornography images and videos trafficked through them – but because they operate as Tor

1 hidden services, the location of the computer servers hosting the websites, and the location and
2 identity of their users who are perpetrating crimes against children, and their child victims, are
3 currently unknown.

4 Stopping the unlawful possession and dissemination of child pornography materials by
5 particular individuals, and rescuing children from the ongoing abuse and exploitation of
6 individual perpetrators, therefore requires more than just shutting down one facility through
7 which such materials are disseminated. Law enforcement must identify and apprehend the
8 perpetrators. Here, the FBI briefly assumed administrative control over an existing facility
9 through which users were already posting and accessing child pornography, for a limited period
10 of time, in order to deploy a court-authorized investigative technique and engage in court-
11 authorized monitoring of user communications, which were necessitated by the particular
12 anonymizing technology deployed by the users of the site, in an effort to identify those
13 perpetrators. This difficult decision, which was disclosed both to the magistrate who approved
14 the NIT and the district judge who approved the Title III monitoring, was amply justified by the
15 particular facts of the investigation.

16 During the government's operation of Website A, regular meetings were held to discuss
17 the status of the investigation and identification of site users and assess whether the site should
18 continue to operate, based upon a balancing of various factors, to include site users' continued
19 access to child pornography, the risk of imminent harm to a child, the need to identify and
20 apprehend perpetrators of those harms to children, and other factors such as those described
21 above. On March 4, 2015, it was determined that the balance of those factors weighed in favor
22 of shutting down the website.

23 **F. Statistics concerning charges**

24 Although it is not reflected in the Court's written order, during the December 11, 2015,
25 hearing the court also stated: "[i]f specifics are not available, I think also the number of charges
26 arising from this investigation should be – the numbers, only numbers, I am saying – should be
27 provided to the defense." Dec. 11, 2015, Tr. at 34. The investigation into users of Website A
28 remains ongoing. To date, at least 137 individuals in the United States are known to have been
charged in connection with the underlying investigation of Website A. That includes thirty-five
individuals who have been determined to be "hands on" child sexual offenders, and seventeen

1 individuals who have been determined to be producers of child pornography. More importantly,
 2 twenty-six child victims have been identified or recovered from abuse. Individual charging
 3 decisions are made at the discretion of United States Attorneys' Offices and/or appropriate state
 4 authorities and this does not represent a complete reporting of all individuals who could be
 5 charged in connection with the investigation.

6 **G. Documents regarding FBI administrative control of Website A**

7 Although the Court also ordered the government to provide: "All documents relating to
 8 review and authorization of the FBI's administrative control of the site by the Department of
 9 Justice or other governmental agencies that were involved in the 'Website A' investigation and
 10 deployment of the NIT at issue in our case," the Court qualified its directive, stating: "Provided
 11 further, that the government need not provide to defense counsel any documents under the above
 12 requirement that constitute reports, memoranda, or other internal government documents made
 13 by an attorney for the government or other government agent in connection with investigating or
 14 prosecuting this case[.] FRCP 16(a)(2)." Dkt. 81 at pp. 2-3.

15 Discovery materials already provided, including the NIT search warrant and the Title III
 16 application paperwork, clearly indicate the scope and purpose of the operation to identify users
 17 who were abusing and exploiting children online while masking their location via the Tor
 18 network. The NIT search warrant affidavit, which clearly described the operation of the website
 19 at a government facility for a limited time in order to identify users, was sworn to by an FBI
 20 Special Agent and presented by an Assistant U.S. Attorney from the Eastern District of Virginia
 21 and a Trial Attorney with the Department of Justice's Child Exploitation and Obscenity Section.
 22 The Title III application and affidavit, which also clearly described the scope and purpose of the
 23 operation, including the website's operation at a government facility for a limited period of time
 24 in order to deploy a court-authorized NIT to identify users, was submitted by two Department of
 25 Justice attorneys, based on an affidavit sworn to by an FBI Special Agent, and approved, as all
 26 Title III applications are required to be, by a Deputy Assistant Attorney General of the
 27 Department of Justice's Criminal Division.

28 Although the United States is in possession of documents that would be responsive to the
 first portion of the Court's order, the United States is not producing those documents at this time
 pursuant to the second portion of the Court's order, Federal Rule of Criminal Procedure 16(a)(2),

1 attorney-client, work product and deliberative process privileges. *See United States v.*
2 *Fernandez*, 231 F.3d 1240, 1246-47 (9th Cir. 2000).

3 DATED this 8th day of January, 2015.

4 Respectfully submitted,

5 ANNETTE L. HAYES
6 United States Attorney

STEVEN J. GROCKI
Chief

7
8 /s/ Matthew P. Hampton

9 Matthew P. Hampton
10 Assistant United States Attorney
11 1201 Pacific Avenue, Suite 700
12 Tacoma, Washington 98402
13 Telephone: (253) 428-3800
14 Fax: (253) 428-3826
15 E-mail: matthew.hampton@usdoj.gov

/s/ Keith A. Becker

Trial Attorney
Child Exploitation and Obscenity
Section
1400 New York Ave., NW, Sixth Floor
Washington, DC 20530
Phone: (202) 305-4104
Fax: (202) 514-1793
E-mail: keith.becker@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that on January 8, 2016, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to the attorney of record for the defendant.

/s/ Matthew P. Hampton
MATTHEW P. HAMPTON
Assistant United States Attorney